Privacy Impact Assessment

System Description

1. **System Name:** Order Online! (NARA Online Ordering System)

2. **System Location:** National Archives and Records Administration (NARA), Archives II facility located in College Park, Maryland.

System Description: Order Online!: Order Online! is a Web-based order entry system that is accessible from NARA's *Archives.gov* site. The public can use Order Online! to request, pay for, and track the status of selected NARA product and service orders that are submitted using the Internet. The system provides an intuitive, easy-to-use interface that supports reproduction requests for copies of select archival records and microfilm publication orders.

The system also incorporates order fulfillment functionality in Order Online! This enables NARA staff and authorized contractors (acting as NARA agents) to track the processing of customer orders. Only payment data is transferred between Order Online! and the Order Fulfillment and Accounting System (OFAS) (See the Glossary descriptions for OFAS and Order Online! for more information.).

Data in the System

1. **Categories of Information Used in the System:**

    a. **Public:** Several types of voluntarily provided information related to the public are used in the system.

        i. **User Profile Information** - includes the following user-provided information: login ID, password, first name, last name, e-mail address [optional], challenge question, and challenge answer. The latter two types of information are used to validate a user's identity for password reset, if needed. Optionally, the user's shipping address, billing address, and credit card information may be stored as part of the user's profile to automatically insert the information in subsequent online orders.

            All user-provided information is securely stored in the Order Online! system according to the General Control stated in Section 3, below. Information about the access to this information is provided in the Access to the Data section.

        ii. **Transaction Information** – includes information related to a specific order that is submitted to NARA via Order Online!, such as item being ordered, shipping recipient and address, credit card number and expiration date, and billing address. This information is passed from Order Online! into OFAS via

an automated XML (Extensible Markup Language) interface within NARA's secure internal network for order fulfillment.

iii. **Order History Information –** includes information related to submitted orders and unfinished orders that may be retained by the customer for short-term reference. Users can access this information with their login ID and password. This information is accessible for up to one year and is in accordance with NARA's Files Maintenance and Records Disposition Data Retention Schedule.

b. Employee: As described above, information is passed directly from Order Online! into OFAS, as such no information related to NARA employees or its agents is used in the system.

c. Other: Non-personal information such as sample images of products and services available for sale, Frequently Asked Questions (FAQs), and the Privacy and Use statement are stored in the system.

2. Sources of Information in the System:

a. NARA Files and Databases: NARA indexes and other related information are used to describe the products (e.g., microfilm publications) and services (e.g., archival material available for reproduction) that can be purchased using Order Online!

b. Federal Agency-Provided Data: Currently, no Federal Agency provides data that is used in the system. In the future, NARA may attempt to acquire usage rights for certain indexes to NARA records that have been created by and are in the custody of other Federal Agencies. These third-party indexes may be used to assist customers in identifying NARA holdings.

c. State and Local Agency-Provided Data: None.

d. Other Third Party Data: Information is collected from a third-party credit card validation service to approve individual credit card transactions before the order is approved and accepted by NARA for fulfillment.

e. Public or NARA Employee Data: Information cited in Data in the System, Section 1.a will be collected from the public. No information is collected from NARA employees.

3. General Controls for Data Integrity to Ensure Integrity (e.g., accuracy, completeness, and validity) of System Data:

Order Online! is a Siebel software application that has built-in controls for data integrity. The accuracy, completeness, and validity of the data is ensured by the software, NARA's extensive test of the application prior to its release into production (following NARA's Systems Development Lifecycle and Configuration Management guidelines), and the Order

Online! Systems Administrator. Through rules established by NARA's Security Officer, the Systems Administrator has implemented security controls to ensure the integrity of the Order Online! data. These controls are evaluated annually as a part of NARA's Certification and Accreditation and Program Self-Audit. The Order Online! Program Manager is responsible for the overall integrity of the system's data. The following also ensures the integrity of Order Online!

a. Data Retention Schedule: NARA Files Maintenance and Records Disposition Manual (FILES 203, Appendix 18, File Number 1807) establishes the data retention schedule for Order Online! In accordance with FILES 203, "documents accumulated by the Trust Fund to record requests from NARA, other Government agencies, and the public for reproduction services or publications of records and other historical documents" (including service orders and related records), should be cut-off after completion of the order and destroyed when one year old. Other records should be destroyed when superseded or obsolete.

The FILES 203 guidance has been implemented according to the following technical specification. Every twelve months, in compliance with FILES 203, 1807-1, a scheduled business service purges the completed order data from the system and permanently destroys it.

For customers who voluntarily choose to store their profile information (e.g., shipping address, billing address, credit card data) in Order Online! for later retrieval, the profile information will remain active in the system until the customer deletes the information using Order Online! or contacts NARA with a request that corresponding data should be deleted. Therefore, in accordance with FILES 203, 1807-3, Order Online! will not expire or inactivate any user accounts or account profile information unless the customer initiates the deletion action.

b. Audit Logs: Order Online! maintains audit logs that track user access to the Order Online! system and records database modifications.

Detailed system logs are maintained for all system processes that run on the Order Online! servers. This includes integration logs that provide details on the orders that are currently sent to OFAS. One log maintains details on the orders that are transferred to OFAS and a second log maintains details on order status updates that are received from OFAS. System logs also report multiple failed login attempts and system administrator updates to the Order Online! environment. System logs are evaluated on a regular basis and are securely backed-up and stored for possible "after-the-fact" reconstruction of performance or security threats. A description of Order Online! and OFAS is provided in the Glossary of Terms.

Order Online! also maintains audit logs that track the status of database or record updates using key system fields: created date, created by, last modified date, last modified by, conflict ID quote number, order number, and order line item number.

i. **Created Date –** the date and time on which a particular record was created in the database. For example, each order in the system stores the date and time the order was created.

ii. **Created By –** the ID of the individual who created a record in the database. For example, the User ID of the person who created an order.

iii. **Last Modified Date –** the date on which the record was last modified. For example, the date when the system updates the order status from "Received" to "Processing".

iv. **Last Modified By –** the User ID of the individual who last modified the record.

v. **Conflict ID –** controls maintained to ensure data integrity in cases where more than one user attempts to access and potentially update the same record in the system.

vi. **Quote Number** – the number associated with a particular quote record in the database. For example, each quote in the system stores the quote number.

vii. **Order Number** – the number associated with a particular order record in the database. For example, each order in the system stores the order number.

viii. **Order Line Item Number** – the number associated with a request line item within a particular order record in the database. For example, each individual request line item within an order in the system stores the order line item number and the business unit assigned to that request line item.

c. **Documentation of Data Elements:** Conceptual and logical data models for Order Online! are documented in the latest release version of the Order Online! Detailed Design Document and the Version Description Document. These data models, in addition to the physical data model, are maintained in NARA's System Architect modeling tool and PVCS configuration management system. All data models were approved by NARA's Data Architect and Data Administrator.

d. **Configuration Management:** The Order Online! production baseline and all subsequent changes (e.g., application, data, infrastructure) are maintained using NARA's configuration management (CM) guidelines, as stated in NARA's Systems Development Lifecycle directive (NARA 805) and supplements to this directive: NARA Information Technology Systems Development Guidelines and Information Technology Systems Development Lifecycle Handbook.

The CM process and supporting tools ensure that planned modifications to Order Online! are fully documented, tested, and approved by relevant business and technical stakeholders. The Order Online! CM Plan and PVCS system are used to support this process.

e. **Service Continuity:** Continuity testing is regularly preformed on Order Online! to ensure that, when unexpected events occur, the critical operations will continue without interruption or will be promptly resumed without impact to critical and sensitive data.

f. **Certification and Accreditation:** Certification and Accreditation (C&A) evaluations are conducted on an annual basis, or as major changes are implemented, to reevaluate the Order Online! system and operational environment as major changes are implemented. A security evaluation study of Order Online! was last completed on August 31, 2005 in accordance with NIST 800-37, "Guidelines for Computer Security Certification and Accreditation."

g. **Program Self-Audit:** Periodically, the program that supports Order Online! initiates a self-audit to ensure compliance with relevant external policy and requirements, internal NARA policy and requirements, and Order Online! procedures. The NARA Security Officer and other relevant staff support the effort to proactively assess compliance and address any identified gaps or issues.

Access to the Data

1. **Who will Have Access to the Data in the System (Users, Managers, System Administrators, Developers, Other)?**

   a. **Users:** Users will have access to their own profile information, if they elect to store this information for later access, as well as order history information. See Categories of Information Used in the System, as described above.

   b. **Managers:** Managers have access to production reports that summarize Order Online! operations (e.g., number of submitted orders, average turnaround time for completed orders, number of new users). These reports do not contain personally identifiable information.

   c. **System Administrator:** The Order Online! System Administrator has access to Order Online! production data, however, encrypted data (e.g., user password and credit card number) cannot be deciphered.

   d. **Developers:** Developers only have access to Order Online! test data, however, a limited number of production developers have access to production data. Access is gained through login ID and password authentication. This access is required for initial data migration and trouble report investigation. Again, encrypted data cannot be deciphered.

2. **How is Data Access Determined?**

   The Order Online! Program Manager is responsible for ensuring that access to Order Online! data is properly controlled throughout the system lifecycle. This oversight ensures that only authorized individuals have access to the system data. The Program Manager, working with the Order Online! integrated project team, follows NARA's Strategic Sequencing Process to

identify and validate data ownership, establish and maintain administrative controls, and define and control access rights.

NARA's information technology projects follow a multi-step process, called the Strategic Sequencing Process, to ensure the proper implementation of new technology capabilities. This process guides NARA's transition from its current state of automation environment (or Baseline Architecture) to its planned state of automation (or Target Architecture), and ensures that each information technology project is properly coordinated with other enterprise initiatives.

Six key steps comprise the process: (1) conduct Business Process Reengineering (BPR) efforts, (2) analyze architectural differences and assess technology maturity, (3) select transition opportunities, (4) define/update architectural implementation plan and projects, (5) define/update Information Resource Management (IRM) project portfolio, and (6) implement projects in accordance with NARA's system development lifecycle.

The highly controlled nature of the Strategic Sequencing Process ensures that team members thoroughly understand the business and technology environment, and that responsible NARA stakeholders are aware of and sign-off on major project milestones. These controls ensure that privacy concerns regarding sensitive data are identified and factored into the system design, user access administration, and ongoing system operations.

3. Are Criteria, Procedures, Controls, and Responsibilities Regarding Access Documented?

Details related to data access, including those stated above, are documented in the latest release version of the Order Online! Concept of Operations, the Order Online! Version Description Document, and the Order Online! System Operations Guide. These documents are updated as the Order Online! system is modified or upgraded.

4. Will users have access to all data on the system or will the users' access be restricted?

Order Online! is a Siebel software application that incorporates numerous access controls that manage the relationship between user roles, user responsibilities (or access rights), and application data views and database records. These access controls, referred to as Siebel "visibility" controls, determine different sets of views and different sets of records that users can see when they log onto Order Online!. These controls ensure that users can see only their own Profile Information, Transaction Information and Order History, in addition to other non-personal information that is stored for user reference (as described above). The System Administrator oversees the different levels of access.

5. What Controls are in Place to Prevent the Misuse of Data by Those Having Access?

There are two primary controls that prevent the misuse of data (e.g., unauthorized browsing) by those who have data access: (1) Data Encryption and (2) NARA Information Technology (IT) Policy. NARA's IT Policy is described in Section 5.b below.

a. **Data Encryption:** The most sensitive data in the Order Online! system are user passwords and user credit card numbers. These data are encrypted as they are created in the system. This data encryption control ensures that those accessing Order Online! data cannot decipher this sensitive information.

b. **NARA IT Policy:** NARA IT Policy is formal guidance that establishes the rules of procedure for the development, implementation, and maintenance of IT systems. This policy includes several components, such as:

   i. **NARA Directives, Supplements, and Interim Guidance -** includes policy guidance such as the Information Technology (IT) Systems Security directive (NARA 804) and its related IT security handbooks that stipulate Management Controls, Operations Controls, Technical Controls, and IT Security Web Page Controls related to NARA systems, support staff, and contractors.

      For example, the policy guidance requires that all system users receive appropriate training, including rules of behavior and consequences for violating the rules. It ensures that NARA maintains an effective incident handling capability (including intrusion detection monitoring and audit log reviews) and that each project adheres to the prescribed incident handling procedures. Additionally, background investigations are conducted on all NARA IT staff and contractors.

   ii. **Certification and Accreditation** – this process, which is conducted annually, or as major changes are implemented, to verify compliance with NARA's IT policies and controls.

   iii. **Inspector General (IG) Audits –** periodically, the IG will conduct an independent audit to review compliance with NARA internal guidelines, external guidelines (e.g., NIST), and program-level procedures and controls.

6. Other Systems that Share Data or Have Access to System Data

a. **What systems share data or have access to system data?** Order Online! passes payment information to the Order Fulfillment and Accounting System (OFAS) for payment processing. The data is transmitted via an automated Extensible Markup Language (XML) interface that operates within NARA's secure internal network. Order status updates are sent back to Order Online! by OFAS to communicate order history and status information to the submitting user.

b. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** NARA's Privacy Officer approves the privacy policy and procedures for Order Online! and is responsible for ensuring compliance with the privacy rights of the public and NARA employees.

7. Other Agency Access to System Data

a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)? No other agency will share data or have access to data in the Order Online! system.

b. How will the data be used by the agency? This is not applicable, as no other agency shares Order Online! data or has access to the Order Online! system.

c. Who is responsible for assuring proper use of the data? There are multiple individuals who are responsible for ensuring the proper use of data: NARA's Privacy Officer, NARA's Chief Information Officer, NARA's Security Officer, Order Online! Program Manager, and Order Online! System Administrator.

d. How will the system ensure that agencies only get the information they are entitled to obtain? This is not applicable, as no other agency shares Order Online! data or has access to the Order Online! system.

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

NARA's Strategic Sequencing Process (see Access to the Data, Section 2) ensures that requirements are properly formulated and tested against the production system. This results in an information architecture that reflects only data that is needed to satisfy the functionality of the system.

2. New Data

a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? The system will not derive new data or create previously unavailable data about an individual through aggregation of other collected data.

b. Will the new data be placed in the individual's record (public or employee)? This is not applicable, as the system will not create or store information about an individual beyond optional profile information (such as user name, billing address and shipping address) that is used to pre-populate information in the online order request.

c. Can the systems make determinations about the public or employees that would not be possible without the new data? The system does not make determinations about the public or NARA employees.

d. How will the new data be verified for relevance and accuracy? Users who choose to store information in their user profile are prompted to review the information prior to

it being saved in the system. Additionally, the user may edit or delete the profile information at any time.

3. Data Consolidation

a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Although statistical reports are used to manage the Order Online! system, there is no consolidation of system data.

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Not applicable.

4. Data Retrieval

a. How will the data be retrieved? Can it be retrieved by personal identification? NARA staff and contractors (acting as authorized agents) access information that is necessary to fulfill, troubleshoot, and ship orders. The information is retrieved by order number or customer name. Only those individuals with approved access rights have this authority and data accessibility.

b. What are the potential effects on the due process rights of the public and employees regarding:

i. Consolidation and Linkage of Files and Systems: Order Online! is an order entry system. There are no perceived effects on the due process rights of the public and NARA employees.

ii. Derivation of Data: Not applicable.

iii. Accelerated Information Processing and Decision Making: Not applicable.

iv. Use of New Technologies: Not applicable.

v. Mitigation of Effects: Not applicable.

Maintenance of Administrative Controls

1. General Controls

a. Explain how the system and its use will ensure equitable treatment of the public and employees. As an online ordering system, there are no impacts regarding the equitable treatment of the public and NARA employees.

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites? Order Online! is operated at one site, and

its data is centrally stored at that site which is located in NARA's College Park, MD facility.

c. **Explain any possibility of disparate treatment of individuals or groups.** As an online ordering system, there is no possibility of disparate treatment of individuals or groups.

2. Data Retention

a. **What are the retention periods of data in this system?** As stated above, order data is retained for a maximum of one year; user profile data is retained as long as the user's account is active in the system.

b. **What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?** The data retention process for Order Online! is described in the Data Retention Schedule section, above. These procedures are also documented in the latest release version of the Order Online! System Operations Guide.

c. **While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?** This is not applicable, as the information is not used to make determinations.

3. Use of New Technology

a. **Is the system using technologies in ways that NARA has not previously employed (e.g., Caller-ID)?** The system incorporates e-commerce functionality that enables users to order and pay for certain NARA products and services in a self-service environment. Previously, NARA customers only had the option of submitting written order requests that contained credit card payment information (or checks). NARA personnel would key the order request and the mode of payment into OFAS for order and payment processing.

b. **How does the use of this technology affect public/employee privacy?** The user of e-commerce technology only automates the customer's ability to submit and pay for NARA products and services. The same data is collected, stored, and administered in a manner that fully protects the user's privacy.

4. Use of Data for Monitoring

a. **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.** The system only captures customer orders for NARA products and services, therefore, it does not provide the capability to identify, locate, or monitor individuals.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain. The system does not provide the capability to identify, locate, or monitor groups of people.

c. What controls will be used to prevent unauthorized monitoring? This is not applicable, as the system does not support or enable monitoring of individuals.

5. System of Record (SOR) Notice

a. Under which SOR notice does the system operate? NARA 37 is the SOR notice for Order Online!.

b. If the system is being modified, will the SOR require amendment or revision? In addition to the Privacy Impact Assessment, the SOR notice will be updated as the Order Online! system is modified or upgraded.

Glossary of Terms

Term	Description
Order Fulfillment and Accounting System (OFAS)	NARA's legacy system that currently supports the customer ordering process: sales and order entry, order fulfillment tracking, and payment processing. **Sales and Order Entry:** OFAS is used in many of NARA's organizational units to process "point of sale" transactions. This includes: • Office of Records Services - Washington, DC; • Office of Presidential Libraries; • Office of the Federal Register; • Office of Regional Records Services; and • National Archives Trust Fund Division. The system is also used by NARA staff and authorized contractors (located in the Washington, DC area) to enter (i.e., receive, maintain control of, and process) reproduction and merchandise orders that are received via the phone or mail. **Order Fulfillment Tracking:** NARA staff and authorized contractors use OFAS to track the processing of phone and mail orders. **Payment Processing:** OFAS bills customers for orders; maintains payment records for orders; processes order payments; and processes refunds. Additionally, OFAS routes customer refunds to the General Services Administration (GSA), which provides NARA's financial and accounting system under a cross-servicing agreement. OFAS records may include: catalogue order forms; other ordering forms; correspondence; copies of checks, money orders, credit card citations, and other remittances; invoices; and order and accounting information in the electronic system. These records may contain some or all of the following information about an individual: name, address, telephone number, record(s) or item(s) ordered, and credit card or purchase order information. OFAS records also include user profile data, reproduction order form data, transaction data, and credit card payment data transmitted from Order Online! (See description, below) via an automated XML (Extensible Markup Language) interface that operates within NARA's secure internal network.
Order Online!	NARA's Web-based order entry system that is accessible from the Archives.gov site. The system enables customers to request, pay for, and track the status of selected NARA product and service orders that are submitted online (that is, via the Web). The system also incorporates order fulfillment functionality in Order Online!, enabling NARA staff and authorized contractors (acting as NARA agents) to track the processing of customer orders. Only payment data is transferred

	between Order Online! and OFAS. Also known as the NARA Online Ordering System.